WPNR 2016/7123 De verplichting tot het bijwerken van onveilige software

Publicatie	WPNR: Weekblad voor Privaatrecht, Notariaat en Registratie
Uitgever	Koninklijke Notariële Beroepsorganisatie
Jaargang	147
Publicatiedatum	22-10-2016
Afleveringnummer	7123
Titel	De verplichting tot het bijwerken van onveilige software

Auteurs	Mr. P.T.J. Wolters, Universitair docent burgerlijk recht en onderzoeker bij het Onderzoekcentrum Onderneming & Recht van de Radboud Universiteit. (p.wolters@jur.ru.nl); Mr. P.W.J. Verbruggen, Universitair docent privaatrecht en onderzoeker bij Tilburg Institute for Private Law (TIP). (Paul.Verbruggen@uvt.nl)

Samenvatting	Een plicht tot het bijwerken van onveilige software kan worden gebaseerd op verschillende open normen. Verschillende argumenten pleiten ervoor om deze plicht bij de ontwikkelaar van de software te leggen.

Paginanummers	832-839
Rubriek	Artikel

WPNR 2016(7123) De verplichting tot het bijwerken van onveilige software

De verplichting tot het bijwerken van onveilige software

Een analyse in het licht van Rb. Amsterdam (vzr.) 8 maart 2016, ECLI:NL:RBAMS:2016:1175 (Consumentenbond/Samsung)

1. Inleiding

'Software'[1] speelt een steeds belangrijkere rol in onze maatschappij. Deze ontwikkeling biedt grote voordelen, maar leidt ook tot het ontstaan van nieuwe risico's. Zij kan bijvoorbeeld leiden tot de onbevoegde verspreiding van persoonlijke informatie en tot cybercrime.[2] Deze risico's ontstaan in het bijzonder als de software geen adequate beveiliging biedt ('onveilig' is). Het voorkomen en repareren van beveiligingslekken is daarom van groot belang. Security updates zijn hierbij een belangrijk hulpmiddel. De ontwikkelaars van software brengen regelmatig updates uit om gebreken in de beveiliging te verhelpen.[3] Zij willen hun product aantrekkelijk houden voor nieuwe en bestaande gebruikers. Zij proberen daarom te voorkomen dat de software bekend komt te staan als onveilig.[4] Daarnaast kunnen andere marktpartijen druk uitoefenen op de ontwikkelaars.[5]

De door de markt opgelegde discipline is echter, vanuit een rechtseconomisch perspectief, zonder juridische verplichting niet optimaal. De keuze om updates te verschaffen is gebaseerd op een analyse van de kosten van het bijwerken van de software en de schade die *de ontwikkelaar* lijdt als hij geen updates uitbrengt. De schade die *anderen*, zoals de gebruikers, door een gebrek in de beveiliging lijden, blijft zonder juridische verplichting buiten beschouwing.[6] Een groot deel van de gebruikers heeft bovendien onvoldoende informatie en kennis om de waarde van een bijgewerkte beveiliging, en de risico's van het gebruik van verouderde software, op een juiste wijze in te schatten en te verdisconteren in de prijs die hij bereid is te betalen.[7] Een juridische plicht tot bijwerken van onveilige software maakt de ontwikkelaar verantwoordelijk voor de schade die anderen lijden als gevolg van een bekend beveiligingslek. De plicht kan hierdoor bijdragen aan het wegnemen van deze inefficiënties.

Een plicht tot het bijwerken van onveilige software blijkt echter niet expliciet uit de Nederlandse wet. Het grootste deel van het Burgerlijk Wetboek bevat geen bijzondere bepalingen voor ‘de digitale wereld’.[8]

Ook de regels die wel met het oog op deze technologische ontwikkelingen zijn ingevoerd, schrijven geen plicht tot updaten voor.[9] Een dergelijke plicht zou wel kunnen worden opgelegd op grond van de in de wet opgenomen open normen. Zolang echter onduidelijk is of en in hoeverre deze normen een verplichting tot het bijwerken van onveilige software in het leven roepen, worden ontwikkelaars onvoldoende geprikkeld om te zorgen voor een adequate beveiliging.[10]

In dit artikel beantwoorden wij de volgende onderzoeksvraag: *in hoeverre is de ontwikkelaar op grond van het Nederlandse privaatrecht verplicht om de beveiliging van onveilige software bij te werken?*

Bij het beantwoorden van deze vraag gaan wij in het bijzonder in op het conflict tussen de Consumentenbond en Samsung (§ 2). Deze focus functioneert tevens als een begrenzing. Deze bijdrage pretendeert geen uitputtende beschrijving te geven van alle mogelijke grondslagen voor een plicht tot het bijwerken van onveilige software.[11] Zij laat slechts zien dat deze plicht op verschillende open normen kan worden gebaseerd. Wij gaan daarnaast alleen zijdelings in op de mogelijkheden om de verplichting door middel van een overeenkomst te beperken en op de plicht in verhoudingen tussen twee professionele partijen. Paragraaf 3 geeft een toelichting van het belang van de verplichting tot het bijwerken van onveilige software. Hierna volgt een overzicht van verschillende mogelijke grondslagen van deze plicht (§ 4). Het artikel eindigt met een conclusie (§ 5).

2. Consumentenbond/Samsung

De onduidelijkheid over het bestaan en de omvang van de plicht tot het bijwerken van onveilige software heeft tot een kort geding tussen de Consumentenbond en Samsung geleid. Dit conflict kan, voor zover van belang in het kader van dit artikel, als volgt worden samengevat.[12] De smartphones van Samsung gebruiken het Android-besturingssysteem. Een door Samsung ontwikkelde ‘softwareschil’ maakt dit systeem geschikt voor een bepaald type telefoon. Ieder model gebruikt een eigen versie van deze schil. Google werkt Android regelmatig bij. Samsung implementeert deze updates echter niet altijd even snel, en soms zelfs helemaal niet. De telefoons blijven hierdoor een verouderde versie van Android gebruiken. Zij zijn daardoor onder andere kwetsbaar voor de volgens Google ‘kritieke’ beveiligingslekken ‘Stagefright’ en ‘Stagefright 2.0’. Deze lekken maken het mogelijk om (op afstand) toegang tot en controle over de telefoons te krijgen.

De Consumentenbond eist in het kort geding (onder andere) dat Samsung de beveiliging van het besturingssysteem van zijn telefoons ten minste twee jaar na de verkoop blijft bijwerken. De voorzieningenrechter wijst de vordering op procestechnische gronden af. Hij komt tot de conclusie dat er geen spoedeisend belang bestaat omdat de gevaren voornamelijk theoretisch zijn en Samsung de software van zijn *nieuwe* modellen, “al dan niet gestimuleerd door de Consumentenbond”, inmiddels heeft bijgewerkt. Hij doet geen inhoudelijke uitspraak over het al dan niet bestaan, en de omvang, van een plicht tot het bijwerken van de beveiliging. De Consumentenbond beraadt zich nog over het nemen van vervolgstappen.

Dit conflict biedt een overzichtelijk vraagstuk. De Consumentenbond eist niet (alleen maar) in algemene zin dat Samsung upgrades of security updates aanbiedt. De bond eist in het bijzonder dat Samsung een bekend, concreet, ‘kritiek’ beveiligingslek oplost. Bovendien staat vast dat Samsung in staat is om dit lek te dichten. Een deel van de modellen is inmiddels immers bijgewerkt. Ten slotte is Samsung voor het herstel niet afhankelijk van andere partijen. De door Google bijgewerkte versie van Android is niet langer kwetsbaar voor Stagefright. Samsung hoeft deze update alleen nog maar te implementeren in zijn softwareschillen.[13] Deze overzichtelijkheid maakt het conflict geschikt als *case study*. Als er in het Nederlandse privaatrecht een plicht tot het bijwerken van onveilige software bestaat, kan deze plicht in ieder geval van toepassing zijn bij bekende, kritieke beveiligingslekken.[14]

3. Het belang van een plicht tot het bijwerken van onveilige software

Dit artikel onderzoekt het bestaan van een juridische plicht tot het *bijwerken* van onveilige software. Een andere benadering is echter ook mogelijk: waarom is de ontwikkelaar niet verplicht om ervoor te zorgen dat zijn product veilig is op het moment dat hij het op de markt brengt?[15] De in paragraaf 4 behandelde open normen zouden ook een plicht om *ex ante* te zorgen voor een passende beveiliging in het leven kunnen roepen. Toch bestaan er praktische bezwaren tegen deze benadering: de plicht kan onvoldoende voorkomen dat de software op een later moment alsnog onveilig blijkt te zijn.

De in paragraaf 4 besproken grondslagen zijn open normen. Hun reikwijdte is afhankelijk van een afweging van de omstandigheden van het geval. Zij verplichten de ontwikkelaar slechts om te zorgen voor een *passende* beveiliging. Het product zal bijvoorbeeld moeten voldoen aan de op het moment van de verkoop bestaande *state-of-the-art.* De normen leiden echter niet tot een plicht om te zorgen voor software die 100% veilig is. De omstandigheid dat de software op een later moment onveilig blijkt te zijn, betekent op zichzelf daarom niet dat de ontwikkelaar zijn plicht heeft geschonden of verwijtbaar heeft gehandeld.[16]

Er bestaan bovendien verschillende praktische en economische obstakels voor het ontwikkelen van veilige software. Allereerst is de meeste moderne software zeer ingewikkeld.[17] Hierdoor is het niet realistisch om een foutloos product te verwachten. Dit besef is ook doorgedrongen tot de jurisprudentie. Zo oordeelde de rechter in Rb. 's-Gravenhage 11 juli 2001, *CR* 2001, p. 268 dat "Voorop gesteld moet worden dat de aard van het geleverde product - nieuwe standaard software - met zich brengt dat dit in zekere mate programmeer- en ontwerpfouten zal bevatten, met name in de eerste versies." Ook de in de ICT-sector gebruikte contracten bevatten dikwijls bepalingen over het bestaan en de omvang van de plicht tot herstel van fouten in de software.[18]

De ontwikkelaar heeft de beveiliging bovendien niet volledig zelf in de hand. De meeste moderne software maakt gebruik van een grote hoeveelheid codes die zijn ontwikkeld door een andere ontwikkelaar. Een fout in een van deze componenten kan de beveiliging van de software aantasten.[19] Zo is ook het Stagefright-lek een gevolg van een programmeerfout in Android, en niet van een fout in de softwareschil van Samsung.

Er bestaat daarnaast een economische prikkel om een product, met of zonder adequate beveiliging, als eerste naar de markt te brengen. Dit speelt in het bijzonder bij software waarvan de waarde afhankelijk is van de gebruikersbasis.[20] Het kan bovendien efficiënter zijn om beveiligingslekken achteraf te dichten.[21] Het is ten slotte mogelijk dat een aanvankelijk goede beveiliging verouderd raakt door technologische ontwikkelingen.[22]

De plicht om onveilige software *ex post* bij te werken functioneert daarom als een noodzakelijke aanvulling op de plicht om *ex ante* te zorgen voor een passende beveiliging. Een ontwikkelaar is tot op een bepaalde hoogte verplicht om ervoor te zorgen dat de software veilig is op het moment dat hij het product naar de markt brengt. Hij dient er bijvoorbeeld voor te zorgen dat er ten tijde van de verkoop geen bekende kritieke beveiligingslekken bestaan. Hij is daarnaast verplicht om lekken te dichten die later ontstaan of aan het licht komen.

4. De juridische grondslag van de plicht om onveilige software bij te werken

Een plicht om onveilige software bij te werken, kan op verschillende grondslagen worden gebaseerd. De Consumentenbond baseert zijn vordering op de plicht tot conformiteit bij koopovereenkomsten (§ 4.1), onrechtmatige daad (§ 4.2) en de Wet Bescherming Persoonsgegevens ('WBP', § 4.3). Wij bespreken deze normen hieronder. Hierbij besteden wij ook aandacht aan gerelateerde gronden.

4.1. Conformiteit bij koopovereenkomsten

4.1.1. Updates als 'eigenschap' van software

De verkoper is op grond van art. 7:17 lid 2 BW verplicht om een 'zaak'[23] te leveren die de eigenschappen bezit die de koper mag verwachten. Gebreken in de geleverde software kunnen tot non-conformiteit

leiden.[24] Een consument mag volgens de Consumentenbond verwachten dat hij een veilige telefoon koopt die twee jaar goed blijft werken. Nu er kritieke beveiligingslekken blijken te bestaan, is Samsung volgens de bond op grond van art. 7:21 lid 1 sub b BW verplicht om de software bij te werken.

Uit paragraaf 3 blijkt echter dat het niet realistisch is om erop te vertrouwen dat de software volledig veilig is. Hoewel een koper mag verwachten dat er op het moment van de verkoop geen bekende kritieke beveiligingslekken bestaan, mag hij er niet op rekenen dat er ook op een later moment geen beveiligingslekken aan het licht komen. Het enkele feit dat op enig moment blijkt dat de telefoons kwetsbaar zijn voor 'Stagefright', maakt de daarvoor verkochte telefoons daarom niet non-conform. Een consument mag in dat geval hoogstens verwachten dat Samsung de beveiliging bijwerkt binnen een redelijke periode na de ontdekking van een kritieke kwetsbaarheid.[25] De relevante eigenschap is in deze benadering niet de ten tijde van de koopovereenkomst bestaande 'beveiliging', maar de 'updates' of 'ondersteuning' die Samsung daarna verschaft. Deze 'eigenschap' is atypisch. De ondersteuning is eerder een bijkomende verplichting van de verkoper dan een kenmerk van de software zelf.[26]

De benadering valt wel binnen een ruime interpretatie van het begrip 'eigenschappen'.[27] Uit de parlementaire geschiedenis blijkt bijvoorbeeld dat ook een garantie kan worden gezien als een eigenschap van de zaak.[28] De verplichting tot het bijwerken vervult een vergelijkbare functie als een garantie dat de software een bepaalde periode veilig zal blijven. Zij beïnvloedt de levensduur (een eigenschap) van de geleverde software.

Dat de plicht tot het bijwerken van onveilige software onder conformiteit kan vallen, wordt verder aannemelijk gemaakt door het Voorstel Richtlijn voor overeenkomsten inzake digitale inhoud, COM (2015) 634 Final. Deze richtlijn formuleert regels voor consumentenovereenkomsten ten aanzien van 'digitale inhoud'. Hieronder valt op grond van art. 2 lid 1 sub a ook software.[29] Uit art. 6 van het voorstel blijkt dat updates van belang zijn voor de conformiteit. De digitale inhoud is op grond van art. 6 lid 1 sub d slechts conform als hij wordt bijgewerkt zoals afgesproken in de overeenkomst. Lid 2 geeft een regel voor het geval dat het contract niet duidelijk maakt op welke manier de inhoud moet worden geüpdatet. De digitale inhoud moet in dat geval geschikt zijn voor de doeleinden waarvoor inhoud van dezelfde omschrijving gewoonlijk zou worden gebruikt. Hij moet onder andere voldoen aan de noodzakelijke toegankelijkheid, continuïteit en veiligheid. Lid 3 bepaalt dat digitale inhoud die gedurende een bepaalde tijd wordt geleverd, de gehele tijd conform moet zijn. Lid 4 stelt ten slotte dat de recentste versie moet worden geleverd tenzij in het contract anders is bepaald.

De eisen die aan de digitale inhoud worden gesteld, zijn onder het voorstel in de eerste plaats afhankelijk van de overeenkomst. De ontwikkelaars kunnen de verplichting om software bij te werken wegschrijven.[30] Het voorstel leidt hierdoor tot een verslechtering van de positie van de consument. Op grond van art. 7:6 BW is art. 7:17 BW in het geval van een consumentenkoop immers van dwingend recht. Wel maakt het voorstel duidelijk dat de eis van conformiteit een verplichting tot het bijwerken van de digitale inhoud in het leven kan roepen. Het benadrukt hiermee de waarde van deze ondersteuning en het belang om haar juridisch te verankeren.

4.1.2. Conformiteit en het bijwerken van onveilige software

De conclusie dat updates onder de werking van de plicht tot conformiteit *kunnen* vallen, betekent nog niet dat de ontwikkelaar ook verplicht is om onveilige software bij te werken. Of dit het geval is, hangt af van de omstandigheden van het geval.[31] Bij de koop van software bestaan er verschillende omstandigheden die voor het aannemen van de plicht pleiten.

Allereerst is het voor de ontwikkelaar relatief gemakkelijk om bekende beveiligingslekken te dichten. Hij heeft de meeste expertise ten aanzien van de software, en kan er met *een* update voor zorgen dat *alle* gebruikers met een veilige versie kunnen werken. Daarnaast moet de ontwikkelaar, als hij de software aantrekkelijk wil houden voor nieuwe gebruikers, het beveiligingsprobleem toch al oplossen. De meeste gebruikers missen daarentegen de expertise om de software te repareren. Zij moeten overschakelen naar een ander product, het beveiligingslek voor lief nemen of, voor zover dit mogelijk is en op individuele basis, hun ICT-systeem op een andere wijze beveiligen. Het ontbreken van ieder recht op updates brengt

de koper bovendien in een onzekere positie. Hij kan niet voorspellen op welke termijn de beveiliging verouderd zal raken. In theorie kan de software een dag na de aankoop waardeloos worden door het bekend raken van een kritiek beveiligingslek.

Verder vormt de omstandigheid dat veel ontwikkelaars security updates uitbrengen (§ 1) een argument voor het aannemen van een voor een gewoonte noodzakelijke algemeen en voortdurend gevolgde gedragslijn. Een juridisch bindende gewoonte vereist echter ook een gedeelde overtuiging dat de ontwikkelaars hiertoe verplicht zijn.[32] Het is niet duidelijk in hoeverre deze overtuiging bestaat.[33] Verschillende auteurs betogen naar aanleiding van het Voorstel Richtlijn voor overeenkomsten inzake digitale inhoud dat een consument ten minste mag verwachten dat de beveiliging gedurende een bepaalde periode wordt bijgewerkt.[34] De Consumentenbond betoogt dat deze termijn bij smartphones ten minste twee jaar moet zijn. Deze periode sluit aan bij de door de UNETO-VNI, de ondernemersorganisatie voor de elektronische detailhandel, gehanteerde verwachte levensduur.[35] De bond gaat zelf uit van een iets langere levensduur.[36] De lengte van abonnementen voor mobiele telefonie vormt een ander argument voor deze periode. Abonnementen voor een bepaalde duur mogen op grond van art. 7.2a lid 7 sub a Telecommunicatiewet voor maximaal 24 maanden worden aangegaan.[37] Een telefoon wordt in veel gevallen in combinatie met een dergelijk abonnement verkocht.[38]

4.1.3. Andere benoemde overeenkomsten en het algemene overeenkomstenrecht

Tot nu toe is ervan uitgegaan dat de software op grond van een koopovereenkomst aan de gebruiker ter beschikking is gesteld. Dit is echter niet altijd het geval. Een overeenkomst tot het ontwikkelen van ‘maatwerk’, of ‘*Software-as-a-Service*’ (SaaS), dient in de meeste gevallen als opdracht te worden gekwalificeerd.[39] Daarnaast betogen verschillende auteurs dat een overeenkomst tot het tijdelijk ter beschikking stellen van software ook als een huurovereenkomst kan worden beschouwd.[40]

Art. 7:17 BW is in deze gevallen niet van toepassing. Wel is de ontwikkelaar van software bij een SaaS-overeenkomst op grond van art. 7:401 BW verplicht om de zorg van een goed opdrachtnemer in acht te nemen.[41] De verhuurder van software is op grond van art. 7:206 lid 1 BW verplicht om gebreken te verhelpen.[42] Een overeenkomst verplicht de ontwikkelaar op grond van art. 6:248 lid 1 BW bovendien, onafhankelijk van de kwalificatie, tot de rechtsgevolgen die uit de gewoonte of de eisen van de redelijkheid en billijkheid voortvloeien. De verplichting om onveilige software bij te werken kan ook op deze artikelen worden gebaseerd. De in paragraaf 4.1.2 besproken argumenten zijn eveneens van belang in de context van deze grondslagen. De kwalificatie van de overeenkomst is daarom niet van doorslaggevende betekenis.[43]

4.2. Onrechtmatige daad

4.2.1. Maatschappelijke zorgvuldigheid

De in paragraaf 4.1 besproken grondslagen ontstaan op grond van een overeenkomst. Zij binden de ontwikkelaar in beginsel alleen ten opzichte van zijn contractspartijen. In veel gevallen kopen de consumenten hun smartphones echter niet direct van Samsung, maar van een elektronicawinkel of een aanbieder van abonnementen voor mobiele telefonie. In deze situatie kunnen zij alleen de tussenschakel, en niet Samsung, aanspreken op grond van de in paragraaf 4.1 besproken grondslagen.

De tussenschakel is, net als Samsung, als verkoper verplicht tot conformiteit. Hij kan daarna Samsung aanspreken op grond van art. 7:25 lid 1 BW. Deze methode heeft verschillende nadelen. Allereerst blijft de consument met lege handen staan als zijn contractspartij failliet gaat of om een andere reden niet kan worden gedwongen om te presteren. De tussenschakel is bovendien niet in staat om de software zelf bij te werken. Alleen Samsung kan dit doen. De consument zou daarom genoegen moeten nemen met ontbinding of een financiële compensatie.

De Consumentenbond spreekt Samsung daarom ook aan op grond van een schending van de maatschappelijke zorgvuldigheid van art. 6:162 BW. De invulling van deze open norm is afhankelijk van de omstandigheden van het geval. De in paragraaf 4.1.2 besproken argumenten kunnen ook hier een rol

spelen.[44] Bovendien weet Samsung dat de door de tussenschakel gekochte smartphones worden doorverkocht. Het is voor het bedrijf kenbaar dat de consumenten belang hebben bij een adequate beveiliging.[45] Samsung moet redelijke maatregelen nemen om te voorkomen dat de gebruikers schade leiden door een gebrek in de beveiliging.[46] De Consumentenbond stelt daarom dat het bedrijf ook zonder overeenkomst ten opzichte van de consumenten verplicht is om het besturingssysteem bij te werken in het geval van een kritiek beveiligingslek. Hij eist nakoming van deze plicht.

4.2.2. Oneerlijke handelspraktijken

De Consumentenbond stelt daarnaast dat Samsung zich schuldig maakt aan misleidende handelspraktijken, onder andere[47] omdat het bedrijf zijn potentiële klanten niet of onduidelijk informeert over de updates die het na de koop ter beschikking stelt. Samsung geeft slechts aan dat het algemene beleid is dat een toestel ongeveer een tot drie jaar software-ondersteuning krijgt en dat de updates 'regelmatig' en 'zo snel mogelijk' beschikbaar worden gesteld. Het bedrijf benadrukt echter dat het geen concrete beloftes kan maken. Volgens de bond geeft Samsung hiermee onvoldoende duidelijk aan van welke smartphones de beveiliging wordt bijgewerkt en hoe lang dit zal gebeuren.

Een handelspraktijk is op grond van art. 6:193d lid 2 BW misleidend, en dus op grond van art. 6:193b BW oneerlijk en onrechtmatig, als essentiële informatie die de gemiddelde consument nodig heeft om een geïnformeerd besluit te nemen, wordt weggelaten en de consument hierdoor een besluit over een transactie neemt of kan nemen dat hij anders niet had genomen. Op grond van art. 6:193e sub a BW vallen bij een uitnodiging tot aankoop, zoals op de website van Samsung, de voornaamste kenmerken van een product onder 'essentiële informatie'. De beveiliging behoort volgens de Consumentenbond tot de voornaamste kenmerken van een smartphone. Bovendien noemt art. 6:193c lid 1 sub b BW de 'klantenservice' als een van de voornaamste kenmerken van een product. De bond stelt daarom dat informatie over de periode waarin en de frequentie waarmee de beveiliging wordt bijgewerkt als essentiele informatie moet worden gekwalificeerd.

Deze stelling is verdedigbaar. De periode waarin en de frequentie waarmee de beveiliging wordt bijgewerkt is van belang voor de levensduur van software. Zij beïnvloedt de termijn waarin het veilig is om het product te gebruiken. Dit geldt in het bijzonder bij smartphones, aangezien een beveiligingslek in dat geval kan leiden tot de verspreiding of het verlies van een grote hoeveelheid vertrouwelijke informatie. Een gemiddelde, en dus 'redelijk geïnformeerde, omzichtige en oplettende',[48] consument heeft deze informatie daarom nodig om een geïnformeerd besluit over de aankoop van een telefoon te kunnen nemen.

De Consumentenbond eist dat Samsung de consumenten informeert over de periode waarin en de frequentie waarmee de beveiliging wordt bijgewerkt. Het bedrijf kan de onrechtmatigheid echter ook wegnemen door de beveiliging gedurende een lange periode frequent te blijven bijwerken. In dat geval bestaat er geen causaal verband tussen de omissie en het besluit om de telefoon aan te schaffen. Een gemiddelde consument die een smartphone wil kopen, zal hier immers niet van afzien als hij te horen krijgt dat de beveiliging een lange tijd zal worden bijgewerkt.

Voor zover Samsung wel informatie verstrekt, mag deze op grond van art. 6:193c lid 1 BW niet feitelijk onjuist of misleidend zijn. Het bedrijf handelt onrechtmatig als het ten onrechte stelt of impliceert dat het de beveiliging gedurende een bepaalde tijd, en met een bepaalde frequentie, blijft bijwerken. Samsung kan de onrechtmatigheid echter wegnemen door het besturingssysteem te updaten. Aanvankelijk onjuiste of misleidende informatie kan hierdoor leiden tot een *de facto* plicht tot updaten.

4.3. Wet bescherming persoonsgegevens

De Consumentenbond baseert zijn vordering ten slotte op art. 13 WBP. Dit artikel, dat op 25 mei 2018 zal worden vervangen door art. 32 Verordening 2016/679/EU (Algemene Verordening Gegevensbescherming, 'AVG'), verplicht de 'verantwoordelijke'[49] tot het nemen van maatregelen die een passend beveiligingsniveau garanderen. Samsung is volgens de bond een verantwoordelijke, aangezien het bedrijf 'persoonsgegevens'[50] van de gebruikers van de smartphones verzamelt.

Wat een passend beveiligingsniveau is, hangt onder andere af van de stand van de techniek, de kosten van de maatregelen en de risico's voor de 'betrokkenen'.[51] De enkele omstandigheid dat de telefoons kwetsbaar blijken te zijn voor het Stagefright-lek, leidt dus niet tot de conclusie dat Samsung zijn plicht heeft geschonden.[52] Wel is het bedrijf volgens de Consumentenbond verplicht om de beveiliging binnen een redelijke termijn alsnog te verbeteren. Volgens de bond stelt het beveiligingslek criminelen in staat om toegang te krijgen tot de via de telefoon verwerkte persoonsgegevens. De Consumentenbond maakt hiermee echter niet duidelijk of het ook mogelijk is om via het Stagefright-lek toegang te krijgen tot de persoonsgegevens die *door Samsung* worden verwerkt. De telefoonnummers die een gebruiker op zijn telefoon opslaat, zijn bijvoorbeeld persoonsgegevens. Het is echter de gebruiker, en niet Samsung, die hiervoor de verantwoordelijke is. De bond stelt slechts dat Samsung 'bepaalde statistische gegevens' verzamelt. Hij maakt echter niet duidelijk of het via het Stagefright mogelijk is om ook deze gegevens in te zien.

Hoewel de uitspraak niet duidelijk maakt of art. 13 WBP in het conflict tussen Samsung en de Consumentenbond van toepassing is, vormt de norm wel degelijk een mogelijke grondslag voor de verplichting tot het bijwerken van onveilige software. Een passend beveiligingsniveau vereist in de meeste gevallen geen volledig veilige software. Het oplossen van bekende beveiligingslekken is echter een relatief doelgerichte manier om een direct gevaar weg te nemen. Deze plicht rust alleen op de ontwikkelaar van software als hij de persoonsgegevens op enige wijze 'verwerkt'.[53] Dit is bijvoorbeeld het geval bij applicaties die gebruik maken van de persoonsgegevens van de gebruikers, zoals Facebook, Tinder en Strava.

5. Conclusie

In dit artikel beantwoorden wij de volgende onderzoeksvraag: *in hoeverre is de ontwikkelaar op grond van het Nederlandse privaatrecht verplicht om de beveiliging van onveilige software bij te werken?* Verschillende grondslagen kunnen een verplichting tot het bijwerken van onveilige software in het leven roepen. Deze verplichting kan voortvloeien uit de plicht tot conformiteit (§ 4.2), de maatschappelijke zorgvuldigheid (§ 4.2.1) en de verwerking van persoonsgegevens (§ 4.3). De ontwikkelaar van software kan bovendien verplicht zijn om (duidelijke) informatie over zijn updatebeleid te verschaffen (§ 4.2.2).

Verschillende argumenten pleiten voor het aannemen van een plicht tot het bijwerken van onveilige software. De grote rol van ICT en internet leidt ertoe dat het belang van een adequate beveiliging significant is. Hoewel de beveiliging van software in de praktijk regelmatig wordt bijgewerkt, is de door de markt opgelegde discipline niet optimaal (§ 1). Praktische en economische obstakels zorgen er bovendien voor dat het niet realistisch is om te verwachten dat de software volledig veilig is. Updates zijn daarom een belangrijk instrument voor het realiseren van een adequate beveiliging (§ 3). De ontwikkelaar is het beste in staat om de beveiligingslekken te dichten (§ 4.1.2). Hij heeft de meeste expertise ten aanzien van zijn software. Bovendien moet hij, als hij de software wil blijven aanbieden, de beveiliging toch al bijwerken. Het ligt daarom voor de hand om de plicht tot het updaten bij de ontwikkelaar te leggen, ook als hij geen overeenkomst heeft met de gebruiker (§ 4.2).

Hiermee is echter niet gegeven dat de plicht in een concreet geval ook echt bestaat. De verplichting tot conformiteit, de zorg van een goed opdrachtnemer, de redelijkheid en billijkheid, de maatschappelijke zorgvuldigheid en het passende beveiligingsniveau zijn open normen. Hun invulling is afhankelijk van de omstandigheden van het concrete geval. De normen stellen het Nederlandse privaatrecht op deze manier in staat om rekening te houden met de bijzonderheden van 'de digitale wereld'.[54] In het geval van een juridisch conflict is het echter uiteindelijk aan de rechter om te bepalen of er een verplichting tot het bijwerken van de beveiliging bestaat en, zo ja, hoe lang en hoe snel de software moet worden geüpdatet. Het conflict tussen Samsung en de Consumentenbond zet deze vragen op de agenda. Onze bijdrage maakt duidelijk dat de plicht tot het bijwerken van onveilige software op verschillende manieren kan worden ingepast in het Nederlandse recht. Zij laat daarnaast zien dat er sterke argumenten bestaan om deze verplichting aan te nemen. De verdere kristallisatie van deze plicht vereist nadere aandacht in de wetenschap en de rechtspraktijk.

In dit artikel gebruiken wij het woord ‘software’ om te verwijzen naar alle vormen van computerprogrammatuur. Het verwijst onder andere naar applicaties, besturingssystemen, firmware en de programmatuur van apparaten die zijn aangesloten op het internet der dingen.

2

Zie voor een beschrijving van de voordelen en risico’s bijvoorbeeld A. Arora, J.P. Caulkins & R. Telang, ‘Sell First, Fix Later: Impact of Patching on Software Quality’, *Management Science* (52) 2006, p. 465; B.C. Kim, P.-Y. Chen & T. Mukhopadhyay, ‘The Effect of Liability and Patch Release on Software Security: The Monopoly Case’, *Production and Operations Management* (20) 2011, p. 603; E. Koops e.a., ‘Inleiding. Hanteerbaar privaatrecht in een digitale wereld’, in: E. Koops e.a. (red.), *Digitaal privaatrecht*, Den Haag: Boom Juridische uitgevers 2014, p. 7-9; T.F.E. Tjong Tjin Tai e.a., Duties of care and diligence against cybercrime, Tilburg: Tilburg University 2015, p. 13; Centraal Planbureau (m.m.v. Nationaal Cyber Security Centrum), *Risicorapportage Cyberveiligheid Economie*, 2016, p. 1-3 en 35-47.

3

Arora, Caulkins & Telang 2006, p. 465; Kim, Chen & Mukhopadhyay 2011, p. 604; D.R. Thomas, A.R. Beresford & A. Rice, ‘Security Metrics for the Android Ecosystem’, in: *ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices* 2015, p. 1; Nationaal Cyber Security Centrum, *Cybersecuritybeeld Nederland*, 2015, p. 10 en 50; Centraal Planbureau 2016, p. 18; V. Mak, *The new proposal for harmonised rules on certain aspects concerning contracts for the supply of digital content* (studie voor het Europees Parlement), PE 536.494, 2016, p. 16.

4

F.M. Nicastro, *Security Patch Management*, Boca Raton, FL: CRC Press 2011, p. 7-8 en 22; Tjong Tjin Tai e.a. 2015, p. 57; B.P.F. Jacobs, ‘Aftercare for the internet of things’, *CSR Magazine* 2016-2, p. 61. Vergelijk in de context van meldplichten T. Moore & R. Anderson, *Economics and Internet Security: a Survey of Recent Analytical, Empirical and Behavioral Research*, TR-03-11, Cambridge, Massachusetts: Harvard University 2011, p. 12; T.F.E. Tjong Tjin Tai, ‘Aansprakelijkheid bij datalekken’, *WPNR* 7110/2016, p. 459.

5

Kim, Chen & Mukhopadhyay 2011, p. 604; Tjong Tjin Tai e.a. 2015, p. 36. Zie voor een voorbeeld in het kader van Android ook www.bloomberg.com/news/articles/2016-05-25/ google-steps-up-pressure-on-partners-tardy-in-updating-android (laatst bezocht op 29 juli 2016). Google zou een lijst hebben opgesteld waarin de fabrikanten van telefoons worden gerangschikt op de snelheid waarmee ze updates van Android doorvoeren. Het bedrijf zou gedreigd hebben om deze lijst openbaar te maken.

6

Kim, Chen & Mukhopadhyay 2011, p. 603; Moore & Anderson 2011, p. 1-3 en 22; Lodder & Toet 2013, p. 137; Centraal Planbureau 2016, p. 15 en 20-21; Jacobs 2016, p. 61.

7

Kim, Chen & Mukhopadhyay 2011, p. 613-614; Thomas, Beresford & Rice 2015, p. 1 en 11; Tjong Tjin Tai e.a. 2015, p. 166; Centraal Planbureau 2016, p. 4, 12 en 16.

8

Koops e.a. 2014, p. 9-10; T.F.E. Tjong Tjin Tai, ‘Privaatrecht voor de homo digitalis’, in: E.M.L. Moerel e.a., *Homo Digitalis* (Preadviezen NJV 2016), Deventer: Wolters Kluwer 2016, p. 251.

9

Zie bijvoorbeeld afdeling 3.1.1A en 6.3.4A BW. Vergelijk echter het in § 4.1.1 besproken Voorstel Richtlijn voor overeenkomsten inzake digitale inhoud, COM (2015) 634 Final en § 4.3.

10

Vergelijk Tjong Tjin Tai e.a. 2015, p. 57. Wij geven enkele voorbeelden. Uit R. Verdult, F.D. Garcia & B. Ege, 'Dismantling Megamos Crypto: Wirelessly Lockpicking a Vehicle Immobilizer', in: USENIX, *Supplement to the Proceedings of the 22nd USENIX Security Symposium*, Washington, DC: USENIX 2013 blijkt dat het door een gebrek in de beveiliging van de elektronische startonderbreker mogelijk is om de auto's van verschillende merken zonder de sleutel te starten. Volkswagen reageerde hier niet op door de beveiliging bij te werken. In plaats daarvan blokkeerde het bedrijf de publicatie van het onderzoek. *Volkswagen v Garcia*, [2013] EWHC 1832 (Ch). Uit E. Novella Lorente, C. Meijer & R. Verdult, 'Scrutinizing WPA2 Password Generating Algorithms in Wireless Routers', *9th USENIX Workshop on Offensive Technologies* 2015 blijkt dat het standaardwachtwoord van bepaalde routers op een eenvoudige manier kan worden achterhaald. KPN, Tele2 en Ziggo gebruiken ondertussen veilige routers, maar vervangen (de beveiliging van) de bestaande exemplaren niet. Wel adviseren zij hun klanten om een eigen wachtwoord in te stellen. http://nos.nl/nieuwsuur/artikel/2051332-reacties-kpn-tele2-en-ziggo.html (laatst bezocht 27 juli 2016). Dit lost het probleem echter niet geheel op, aangezien de routers kunnen terugschieten naar de fabrieksinstellingen.

11

Zie voor een overzicht van de relevante normen P.W.J. Verbruggen e.a., 'Towards Harmonised Duties of Care and Diligence in Cybersecurity', in: Cyber Security Council (red.), *European Foresight Cyber Security Meeting 2016*, 2016, p. 78-108.

12

Rb. Amsterdam (vzr.) 8 maart 2016, ECLI:NL:RBAMS: 2016:1175. De dagvaarding en pleitnota zijn beschikbaar op www.consumentenbond.nl/campagnes/updaten/kort-geding/ (laatst bezocht 28 juli 2016). Zie over deze zaak ook P.W.J. Verbruggen, 'Van de redactie', *TvC* 2016, p. 97-98.

13

In een deel van de gevallen moet de update worden doorgegeven door de aanbieders van mobiele telefonie. Deze situatie blijft verder onbesproken, ook omdat zij niet afdoet aan de verplichting van Samsung.

14

In het navolgende veronderstellen wij dat het lek bestaat en kritiek is.

15

Updates kunnen in deze benadering worden beschouwd als maatregelen om de uit de schending van deze plicht voortvloeiende schade te beperken. Vergelijk College Bescherming Persoonsgegevens 15 januari 2013, *JBP* 2014, 54; Kim, Chen & Mukhopadhyay 2011, p. 603 en 609.

16

Vergelijk ook Tjong Tjin Tai e.a., p. 56-57. Verwijtbaarheid is een van de gronden voor het aannemen van toerekenbaarheid op grond van de art. 6:75 en 162 lid 3 BW.

17

Kim, Chen & Mukhopadhyay 2011, p. 607; Tjong Tjin Tai e.a. 2015, p. 33-37.

18

Zie bijvoorbeeld Nederland ICT voorwaarden 2014, in het bijzonder art. 25.1; Rb. Midden-Nederland 4 mei 2016, ECLI:NL:RBMNE:2016:2195. Deze voorbeelden zien niet specifiek op het herstel van een beveiligingslek.

19

Tjong Tjin Tai e.a. 2015, p. 33-34. Zie voor enkele voorbeelden Nationaal Cyber Security Centrum 2015, p. 50; Centraal Planbureau 2016, p. 17.

20

Kim, Chen & Mukhopadhyay 2011, p. 616; Moore & Anderson 2011, p. 3; A.R. Lodder & J. Toet, 'Cybersecurity: Europese Unie initiatieven voor een intrinsiek grensoverschrijdend fenomeen', *IR* 2013, p. 137; Tjong Tjin Tai e.a. 2015, p. 34-35 en 166.

21

Vergelijk Arora, Caulkins & Telang 2006, p. 466; Kim, Chen & Mukhopadhyay 2011, p. 610. De verhouding tussen de schade en de kosten van de voorzorgsmaatregelen is ook van belang voor de vraag of de ontwikkelaar onrechtmatig handelt. HR 5 november 1965, *NJ* 1966, 136 (*Kelderluik*).

22

Pseudonimisatie door middel van '*hashing*' kan bijvoorbeeld worden gekraakt door middel van brute computerkracht. Article 29 Data Protection Working Party, *Opinion 05/2014 on Anonymisation Techniques*, 0829/14/EN WP216, 2014, p. 20. Een toename van de beschikbare computerkracht kan ertoe leiden dat de aanvankelijke adequate pseudonimisatie op een later moment te makkelijk te kraken is.

23

De bepalingen van titel 7.1 BW zijn op grond van de art. 7:5 lid 5 en 47 BW en HR 27 april 2012, *NJ* 2012, 293 (*Beeldbrigade/Hulskamp*) ook van toepassing op de koop van standaardsoftware. Zie ook W.F.R. Rinzema, 'Kwaliteit en software: een goede zaak', *CR* 2012, p. 100-104; E.D.C. Neppelenbroek, 'Een koopfictie in een fictieve wereld. De hanteerbaarheid van het kooprecht voor digitale inhoud in het CESL', in: E. Koops e.a. (red.), *Digitaal privaatrecht*, Den Haag: Boom Juridische uitgevers 2014, p. 161; J.L. Jonker & J.A. Bal, 'Toepasselijkheid huurtitel 7.4 BW op IT', *CR* 2015, p. 191-192.

24

Rb. 's-Gravenhage 11 juli 2001, *CR* 2001, p. 268; Rinzema 2012, p. 103 (in de context van een gebrekkige beveiliging); Neppelenbroek 2014, p. 154. Volgens Tjong Tjin Tai e.a. (2015, p. 55-56) vallen beveiligingslekken van software niet onder non-conformiteit omdat zij het normale gebruik van software niet verhinderen. Zij leiden slechts tot onwenselijke neveneffecten. Deze stelling is onjuist. Het ontbreken van de eigenschappen die nodig zijn voor normaal gebruik is geen vereiste voor het toepassen van art. 7:17 BW. Ook als de zaak op een andere manier afwijkt van de overeenkomst of eigenschappen mist die de koper mag verwachten, is er sprake van non-conformiteit. HR 23 november 2007, *NJ* 2008, 552 (*Ploum/Smeets en Geelen I*); *Parl. Gesch. Boek 7*, p. 125 (M.v.A. II); Asser/Hijma (*7-I**) 2013, nr. 333 en 343.

25

Vergelijk Rb. Midden-Nederland 30 maart 2016, C/16/344721 / HA ZA 13-387, waar in een conflict tussen professionele partijen een vergelijkbaar resultaat werd behaald. De koper kreeg wel een security

update, maar had geen recht op vergoeding van de kosten die hij door het gebrek in de beveiliging heeft gemaakt

26

Vergelijk C. Wendehorst, *Sale of goods and supply of digital content - two worlds apart?* (studie voor het Europees Parlement), PE 556.928, 2016, p. 14.

27

HR 8 juli 2011, *NJ* 2013, 256 (*IJsseloevers/De Jong*) (goodwill is een eigenschap van een onderneming); Asser/Hijma (*7-I**) 2013, nr. 334; M.M. van Rossum, *GS bijzondere overeenkomsten*, art. 7:17, aantekening 1. Zie ook art. 6:193c lid 1 sub b BW, besproken in § 4.2.2.

28

Parl. Gesch. Boek 7, p. 120 (M.v.T.); Asser/Hijma (*7-I**) 2013, nr. 339; M.M. van Rossum, *GS bijzondere overeenkomsten*, art. 7:17, aantekening 5 en 18.

29

De precieze reikwijdte van de richtlijn is niet helder. Overweging 17 stelt dat de bijzondere aspecten van het internet der dingen apart worden geregeld. Overweging 11 bepaalt dat de richtlijn niet van toepassing is "op digitale inhoud die zodanig in goederen is verwerkt dat deze inhoud als een integrerend deel van die goederen functioneert en de functies ervan aan de hoofdfuncties van de goederen ondergeschikt zijn". Het is niet altijd eenvoudig om te bepalen of de geïntegreerde software ondergeschikt is aan de hoofdfunctie. M.B.M. Loos, 'Europese harmonisatie van online en op afstand verkoop van zaken en de levering van digitale inhoud (II)', *NtEr* 2016, p. 150; Mak 2016, p. 7-9; Wendehorst 2016, p. 6-8. Bij een smartphone is het geïntegreerde en op maat gemaakte besturingssysteem zo belangrijk dat een dergelijke ondergeschiktheid niet voor de hand ligt.

30

H. Beale, *Scope of application and general approach of the new rules for contracts in the digital environment* (studie voor het Europees Parlement), PE 536.493, 2015, p. 20-21; Loos 2016, p. 152; Mak 2016, p. 15; R. Manko, ? *Contracts for supply of digital content* (studie voor het Europees Parlement), PE 582.048, 2016, p. 1 en 17-18.

31

HR 23 november 2007, *NJ* 2008, 552 (*Ploum/Smeets en Geelen I*); HR 21 mei 2010, *NJ* 2010, 275 (*Korea Trade/Im-pro*); *Parl. Gesch. Boek 7*, p. 121 (N.v.W. 1) en 125 (M.v.A. II); Asser/Hijma (*7-I**) 2013, nr. 335.

32

Asser/Scholten 1974 (*Algemeen deel**), p. 106-107; P.T.J. Wolters, *Alle omstandigheden van het geval* (diss. Nijmegen, Serie Onderneming & Recht deel 77), Deventer: Kluwer 2013, p. 75-76; Asser/Hartkamp & Sieburgh 2014 (*6-III*), nr. 382; Asser procesrecht/Veegens/Korthals Altes & Groen 2015 (*7*), nr. 121.

33

Tjong Tjin Tai e.a. 2015, p. 57.

34

Beale 2015, p. 27; Loos 2016, p. 153; Mak 2016, p. 17; Manko 2016, p. 33-34.

35

www.uneto-vni.nl/stream/flyer-gebruiksduurverwachting (laatst bezocht 22 juli 2016).

36

I. Joris, 'Lang leve de levensduur', *DigitaalGids* 2016-3, p. 22.

37

Tot 1 oktober 2016: art. 7.2a lid 2 Telecommunicatiewet.

38

Zie over de juridische complicaties bij deze overeenkomsten ook HR 12 februari 2016, *RvdW* 2016, 279.

39

Rb. Arnhem 7 december 2011, ECLI:NL:RBARN:2011: BU9785; Rinzema 2012, p. 104; Jonker & Bal 2015, p. 192.

40

T. Burgers, 'Software as a Service en het huurrecht', *IR* 2011, p. 107-110; Jonker & Bal 2015, p. 192.

41

Rinzema 2012, p. 105. De zorg van een goed opdrachtnemer is een kristallisatie van de redelijkheid en billijkheid en daarom afhankelijk van de omstandigheden van het geval. Zie hierover Wolters 2013, p. 15.

42

Burgers 2011, p. 109-110; Jonker & Bal 2015, p. 193-194.

43

Vergelijk Rinzema 2012, p. 105. De kwalificering oefent wel invloed uit op de mogelijkheden om de plichten contractueel te beperken. Zie de art. 7:6 en 209 BW.

44

Vergelijk V. van den Brink, 'Redelijkheid en billijkheid en hun overlap met verwante wettelijke bepalingen', *MvV* 2012, p. 23; Wolters 2013, p. 18-19; Asser/Hartkamp & Sieburgh (*6-IV*) 2015, nr. 76. Zie ook § 4.1.3.

45

Vergelijk HR 24 april 1992 *NJ* 1993, 643 en 644 (*Van Wijngaarden/Nederland*); HR 10 december 1993, *NJ* 1994, 667 (*Van Ittersum/Rabobank*); HR 24 september 2004, *NJ* 2008, 587 (*Vleesmeesters/Alog*); HR 20 januari 2012, *NJ* 2012, 59 (*Wierts/Visseren*); C.J.H. Jansen & A.J. van der Lely, '(Buiten)contractuele aansprakelijkheid voor onjuiste mededelingen: een vergelijking van Engels, Duits en Nederlands recht', *TVVS* 1998, p. 47; E.J.A.M. van den Akker, *Beroepsaansprakelijkheid ten opzichte van derden. Een rechtsvergelijkend onderzoek naar de zorgplichten van accountants, advocaten en notarissen ten*

opzichte van anderen dan hun opdrachtgever (diss. Tilburg), Den Haag: Boom Juridische uitgevers 2001, p. 31-35; Wolters 2013, p. 244.

46

Vergelijk HR 5 november 1965, *NJ* 1966, 136 (*Kelderluik*); Asser/Hartkamp & Sieburgh (*6-IV*) 2015, nr. 58.

47

Zie de dagvaarding voor een uitgebreidere bespreking van de handelspraktijken die volgens de Consumentenbond misleidend zijn.

48

Zie over dit criterium HvJ EG 16 juli 1998, nr. C-210/96, ECLI:EU:C:1998:369; Overweging 18 richtlijn 2005/29/ EG (oneerlijke handelspraktijken); D.W.F. Verkade, *Oneerlijke handelspraktijken jegens consumenten* (Monografieën BW deel B49a), Deventer: Kluwer 2009, p. 31; C.M.D.S. Pavillon, *Open normen in het Europees consumentenrecht. De oneerlijkheidsnorm in vergelijkend perspectief* (diss. Groningen, Serie Recht en Praktijk deel CR4), Deventer: Kluwer 2011, p. 297-302.

49

Degene die het doel en de middelen voor de verwerking van de persoonsgegevens vaststelt. Zie over dit begrip de art. 1 sub d WBP en 4 (7) AVG; Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of "controller" and "processor"*, 00264/10/EN WP 169, 2010.

50

Gegevens over geïdentificeerde of identificeerbare natuurlijke personen. Zie over dit begrip de art. 1 sub a WBP en 4 (1) AVG; Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data*, 01248/07/EN WP 136, 2007.

51

De art. 13 WBP en 32 AVG. De 'betrokkenen' zijn de personen op wie de gegevens betrekking hebben. Zie over dit begrip de art. 1 sub f WBP en 4 (1) AVG.

52

Kamerstukken II 1997/98, 25892, nr. 3, p. 99; College Bescherming Persoonsgegevens, *CBP Richtsnoeren. Beveiliging van persoonsgegevens*, 2013, p. 10.

53

Zie over dit begrip de art. 1 sub b WBP en 4 (2) AVG. Verzamelen is een vorm van 'verwerking'.

54

Zie noot 8.